A4

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-041177
(43)Date of publication of application : 08.02.2002

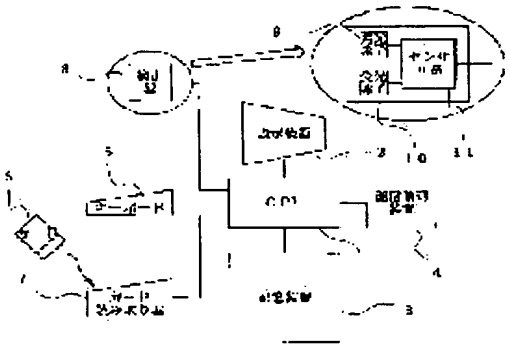
(51)Int.Cl. G06F 1/00
G06F 12/14

(21)Application number : 2000-221813
(22)Date of filing : 24.07.2000

(71)Applicant : TOYO COMMUN EQUIP CO LTD
(72)Inventor : KUROSAWA KAZUO

(54) METHOD AND DEVICE FOR PROTECTING INFORMATION OF COMPUTER

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent a computer from being unauthorizedly used by providing a function for preventing a medium in which personal information is stored from being left.
SOLUTION: This device is provided with a CPU 1 for performing the control of a computer and data processing, a display device 2 for displaying processed results, a storage device 3 for storing various information or arithmetic results or the like, a communication controller 4 to be used at the time of its connection to a network, a keyboard 5 for inputting data or instructions or the like, a card 6 in which personal information such as user ID and password is written, a card reader 7 for reading the information written in the card 6, and a detector 8 for detecting that a computer user is away from his or her seat. Also, the detector 8 is provided with a light emitting element 9 for emitting infrared rays to the computer user, a light receiving element 10 for receiving the infrared rays reflected from the computer user, and a sensor circuit 11 for driving and emitting the light emitting element 9, and detecting the reflected light by being connected to the light receiving element 10.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－41177
（P2002－41177A）
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.'	識別記号	FI	テーマコード'(参考)
Ｇ０６Ｆ　1/00	３７０	Ｇ０６Ｆ　1/00	３７０Ｅ　５Ｂ０１７
	３９０		３９０Ｅ
12/14	３２０	12/14	３２０Ｃ

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願2000－221813(P2000－221813)

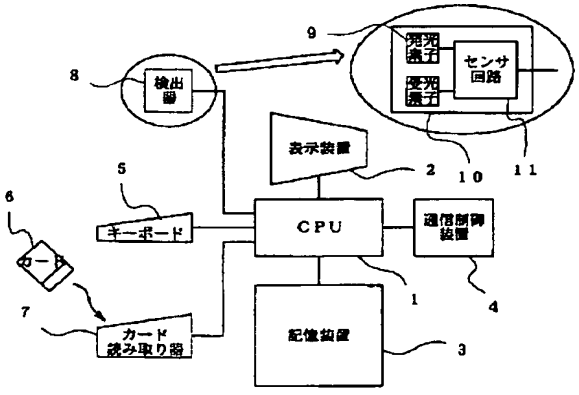
(22)出願日　平成12年７月24日(2000.7.24)

(71)出願人　000003104
東洋通信機株式会社
神奈川県高座郡寒川町小谷２丁目１番１号
(72)発明者　黒沢　和雄
神奈川県高座郡寒川町小谷二丁目１番１号
東洋通信機株式会社内

Ｆターム(参考)　5B017 AA07 BA05 CA00

(54)【発明の名称】　コンピュータの情報保護方法及び装置

(57)【要約】
【課題】個人情報を格納した媒体の放置防止機能を設け、コンピュータの不正使用を防止することを目的とする。
【解決手段】コンピュータの制御及びデータ処理を行なうＣＰＵ１と、処理結果を表示する表示装置２と、種々の情報や演算結果等を格納する記憶装置３と、ネットワークに接続する際に用いられる通信制御装置４と、データ或いは命令等を入力するキーボード５と、ユーザＩＤおよびパスワード等の個人情報が書き込まれたカード６と、カード６に書き込まれた情報を読み込むカード読み取り器７と、コンピュータ使用者の離席を検出する検出器８とにより構成する。又、検出器８は、コンピュータ使用者に対して赤外光を放射する発光素子９と、コンピュータの使用者から反射する赤外光を受光する受光素子１０と、発光素子９を駆動して発光させると共に受光素子１０と接続して反射光を検出するセンサ回路１１とを備えている。



1

【特許請求の範囲】
【請求項１】コンピュータ使用者の個人情報を格納した媒体を設け、該媒体へ書き込まれた内容を読み取り確認することにより前記コンピュータ使用者の使用許可認定を行なうコンピュータの情報保護方法において、
前記個人情報を格納した媒体が読み取り、当該個人情報と管理情報とを整合するステップと、
前記整合の結果、個人情報と管理情報とが整合していた場合にコンピュータ使用者の着席確認を行うステップと、
コンピュータ使用者の着席確認が取れない場合に警報を発するか或いはコンピュータをロックアウトするステップとを含み、
読み取り器に挿入されたまま放置されることにより、該媒体を不正使用したコンピュータへのログインを防止したことを特徴とするコンピュータの情報保護方法。
【請求項２】コンピュータ使用者の個人情報を格納した媒体を設け、該媒体へ書き込まれた内容を読み取り確認することにより前記コンピュータ使用者の使用許可認定を行なうコンピュータの情報保護装置において、
前記個人情報を格納した媒体を読み取る媒体読取手段と、
個人情報を含む管理情報を予め格納する情報格納手段と、
読み取った個人情報と格納された管理情報とを比較する比較手段と、
コンピュータ使用者の着席を確認するための確認手段とを備え、
前記比較の結果、個人情報と管理情報とが整合していた場合に前記確認手段によってコンピュータ使用中にコンピュータ使用者の着席確認を行い、
コンピュータ使用者の着席確認が取れない場合に警報を発するか或いはコンピュータをロックアウトすることにより、前記読み取り手段への媒体放置を防止したことを特徴とするコンピュータの情報保護装置。
【請求項３】前記確認手段は、コンピュータの正面に設けた発光素子からコンピュータ使用者に光を放射し、コンピュータ使用者から反射する前記光を受光センサで検出して、コンピュータ使用者の着席を判別をしたことを特徴とする請求項２記載のコンピュータの情報保護装置。
【請求項４】前記発光素子が赤外線発光ダイオード及び前記受光素子がフォトダイオード或いはフォトトランジスタであることを特徴とした請求項３記載のコンピュータの情報保護装置。
【請求項５】前記確認手段は、コンピュータの正面に設けた撮像素子により撮影し、該撮影画像の変化を検出して、コンピュータ使用者の着席を判別をしたことを特徴とする請求項２記載のコンピュータの情報保護装置。
【請求項６】前記撮像素子がＣＣＤカメラであることを

2

特徴とした請求項５記載のコンピュータの情報保護装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はコンピュータの情報保護方法に関し、特にコンピュータの使用の際に、使用者が正規使用者であるかを特定する方法として、カードを用いて個人情報を管理するコンピュータの情報保護方法に関する。
【０００２】
【従来の技術】従来、コンピュータを使用する際には、記憶装置に書き込まれているデータベース等を不正に取得出来ないよう、或いは、コンピュータをネットワークに接続して不正使用が出来ないようにするため、コンピュータにログインしようとするものが正規の使用者であるかを特定するための操作が必要である。その特定のために、ユーザＩＤ及びパスワード等をログイン時に入力させ、予め登録してあるコンピュータの管理情報と照合して、一致した場合のみコンピュータの使用を許可するようにしている。ユーザＩＤ及びパスワード等のコンピュータへの入力方法として、キーボードからその都度入力する方法の他、磁気カード或るいはＩＣカード等に個人情報を格納し、カード読み取り器に挿入することでデータを読み出して、コンピュータの管理情報と照合することにより一致を確認する方法がある。このカードによる個人情報の入力手段は、使用者にとって、ユーザＩＤ及びパスワード等の記憶やデータの手作業による入力等の煩雑さがなく有効な手段である。
【０００３】図７に、従来から用いられているコンピュータの情報保護方法を示す構成例を示す。同図は、コンピュータの制御及びデータ処理を行なう中央処理装置（以降、ＣＰＵと称す）１と、処理結果を表示する表示装置と、種々の情報や演算結果等を格納する記憶装置３と、コンピュータをネットワークに接続する際に用いられる通信制御装置４と、データ或いは命令等を入力するキーボード５と、ユーザＩＤおよびパスワード等の個人情報が書き込まれた磁気或いはＩＣを用いて構成するカード６と、カード６に書き込まれた情報をコンピュータに読み込むカード読み取り器７とにより構成する。図７の動作を説明すると、先ず、コンピュータの使用者は、コンピュータの電源を投入してコンピュータを起動した後、ユーザＩＤおよびパスワード等の個人情報が書き込まれたカード６を、カード読み取り器７に挿入する。ＣＰＵ１は、読み取った個人情報と、記憶装置３に格納しているコンピュータの管理情報とを照合して、個人情報が登録してある管理情報に該当する場合には、コンピュータにログインさせて使用を許可する。一方、個人情報が登録してある管理情報に該当しない場合は、コンピュータの使用を拒否する。
【０００４】

【発明が解決しようとする課題】しかしながら、従来から用いられているコンピュータの情報保護方法は、個人情報を格納した媒体であるカードにより、ユーザＩＤ及びパスワードの確認を行なうため、カードをカード読み取り器に挿入したまま離席した際に他者に不正利用されることや、不注意からカードを放置して他者に不正使用される等の危険性を伴うという欠点を有していた。本発明は、上述したような従来から用いられているコンピュータの情報保護方法の問題点を解決するためになされたものであって、個人情報を格納した媒体の放置検出機能を設け、コンピュータの不正使用を防止するコンピュータの情報保護方法を提供することを目的とする。

【０００５】

【課題を解決するための手段】上記目的を達成するために本発明に係るコンピュータの情報保護方法及び装置は、以下の構成をとる。請求項１記載のコンピュータの情報保護方法は、コンピュータ使用者の個人情報を格納した媒体を設け、該媒体へ書き込まれた内容を読み取り確認することにより前記コンピュータ使用者の使用許可認定を行なうコンピュータの情報保護方法において、前記個人情報を格納した媒体が読み取り、当該個人情報と管理情報とを整合するステップと、前記整合の結果、個人情報と管理情報とが整合していた場合にコンピュータ使用者の着席確認を行うステップと、コンピュータ使用者の着席確認が取れない場合に警報を発するか或いはコンピュータをロックアウトするステップとを含み、読み取り器に挿入されたまま放置されることにより、該媒体を不正使用したコンピュータへのログインを防止したことを特徴とする。請求項２記載のコンピュータの情報保護装置は、コンピュータ使用者の個人情報を格納した媒体を設け、該媒体へ書き込まれた内容を読み取り確認することにより前記コンピュータ使用者の使用許可認定を行なうコンピュータの情報保護装置において、前記個人情報を格納した媒体を読み取る手段と、個人情報を含む管理情報を予め格納する手段と、読み取った個人情報と格納された管理情報とを比較する手段と、コンピュータ使用者の着席を確認するための確認手段とを備え、前記比較の結果、個人情報と管理情報とが整合していた場合に前記確認手段によってコンピュータ使用中にコンピュータ使用者の着席確認を行い、コンピュータ使用者の着席確認が取れない場合に警報を発するか或いはコンピュータをロックアウトすることにより、前記読み取り手段への媒体放置を防止したことを特徴とする。請求項３記載のコンピュータ保護装置は、請求項２記載の発明において、前記確認手段は、コンピュータの正面に設けた発光素子からコンピュータ使用者に光を放射し、コンピュータ使用者から反射する前記光を受光センサで検出して、コンピュータ使用者の着席を判別をしたことを特徴とする。請求項４記載のコンピュータ保護装置は、請求項３記載の発明において、前記発光素子が赤外線発光ダイオード及び前記受光素子がフォトダイオード或いはフォトトランジスタであることを特徴とする。請求項５記載のコンピュータ保護装置は請求項２記載の発明において、前記確認手段は、コンピュータの正面に設けた撮像素子により撮影し、該撮影画像の変化を検出して、コンピュータ使用者の着席を判別をしたことを特徴とする。請求項６記載のコンピュータ保護装置は請求項５記載の発明において、前記撮像素子がＣＣＤカメラであることを特徴とする。

【０００６】

【発明の実施の形態】以下、図示した実施例に基づいて本発明を詳細に説明する。図１は、本発明に係るコンピュータの情報保護装置の一実施例を示す第一の構成図である。同図は、コンピュータの制御及びデータ処理を行なうＣＰＵ１（比較手段）と、処理結果を表示する表示装置２と、種々の情報や演算結果等を格納する記憶装置３（情報格納手段）と、コンピュータをネットワークに接続する際に用いられる通信制御装置４と、データ或いは命令等を入力するキーボード５と、ユーザＩＤおよびパスワード等の個人情報が書き込まれた磁気或いはＩＣを用いて構成するカード６と、カード６に書き込まれた情報をコンピュータに読み込むカード読み取り器７（媒体読み取り手段）と、コンピュータ使用者が離席していないかどうかの検出を行なう検出器８（確認手段）とにより構成する。又、検出器８は、コンピュータ使用者に対して赤外光を放射する発光素子９と、コンピュータ使用者から反射する赤外光を受光する受光素子１０と、発光素子９を駆動して発光させると共に受光素子１０と接続して反射光を検出するセンサ回路１１とを備えている。又、発光素子９としては、発光ダイオードが、受光素子１０としては、フォトダイオード或いはフォトトランジスタが使用される。

【０００７】図１の動作を説明すると、先ず、コンピュータ使用者は、コンピュータの電源を投入してコンピュータを起動した後、ユーザＩＤ及びパスワード等の個人情報が書き込まれたカード６を、カード読み取り器７に挿入する。ＣＰＵ１は、読み取った個人情報と、記憶装置３に格納しているコンピュータの管理情報とを照合して、個人情報が登録してある管理情報に一致する場合には、コンピュータにログインさせて使用を許可する。一方、個人情報が登録してある管理情報に一致しない場合は、コンピュータの使用を拒否する。又、同一カードの挿入を所定の回数行なっても個人情報と管理情報が一致しない場合は、強制ロックアウト状態としてコンピュータの動作を停止する。次に、コンピュータにログインすると、検出器８が動作を開始し、発光素子９から赤外光を、コンピュータの画面に正対しているコンピュータ使用者に対して放射する。放射した赤外光は、コンピュータ使用者に反射した後、赤外光透過フィルタを介して受光素子１０に入力する。センサ回路１１は、反射光を検

出することにより、検出信号オンをＣＰＵ１に入力し、コンピュータ使用者がコンピュータ席に着席していることを確認する。

【０００８】次に、ＣＰＵ１は、センサ回路１１が反射光を検出できず検出信号をオフとし、コンピュータ使用者がコンピュータ席を離席していることを確認すると、可聴音等により警報を発する。この時、コンピュータ使用者が、一定時間内にコンピュータ席に着席するか、カード６をカード読み取り器７から取り出す等の適切な処置を行なわない場合は、コンピュータを強制的にロックアウトさせ、コンピュータの動作を停止する。尚、停止後のコンピュータは、コンピュータ管理者の操作により復旧させる。

【０００９】図２は、本発明に係るコンピュータの情報保護方法の一実施例を示す第一の外観図で、デスクトップ型コンピュータに実施した例である。同図は、ＣＰＵと記憶装置と通信制御装置とを内蔵したコンピュータ本体１２と、表示装置２と、キーボード５と、カード読み取り器７と、検出器８と、コンピュータ使用者１３とにより構成する。

【００１０】図３は、本発明に係るコンピュータの情報保護方法の一実施例を示す第一の構成図について動作を示すフローチャートである。同図を説明すると、コンピュータ使用者は、コンピュータを起動した後（ステップ１）、カードをカード読み取り器に挿入する（ステップ２）。コンピュータは、カードに書き込まれている個人情報のユーザＩＤが、コンピュータに予め登録してある管理情報と一致するかの判定を行い（ステップ３）、一致していない場合は、カードをカード読み取り器から強制的に排出する（ステップ４）。次に、同一カードの排出回数をカウントし、所定の回数カウントした際は（ステップ５）、ロックアウトに移行してコンピュータの動作を停止する（ステップ６）。一方、一致している場合は、ステップ７に進み、カードに書き込まれている個人情報のパスワードが、コンピュータに予め登録してある管理情報と一致するかの判定を行い、一致していない場合は、カードをカード読み取り器から強制的に排出する（ステップ４）。次に、同一カードの排出回数をカウントし、所定の回数カウントした際は（ステップ５）、ロックアウトに移行してコンピュータの動作を停止する（ステップ６）。一致している場合は、コンピュータにログインして（ステップ８）、利用を開始する（ステップ９）。

【００１１】次に、コンピュータの利用を開始すると、検出器が起動して赤外光をコンピュータ使用者に放射する（ステップ１０）。その赤外光の反射が検出されなくなると（ステップ１１）、コンピュータ使用者がカードをカード読み取り器に挿入したまま離席したことを認識し、可聴音等の警報を発して（ステップ１２）所定の時間内に前記赤外光を再受光するかを検出する（ステップ１３）。そこで、再受光した場合は、コンピュータ利用者の着席を検出してステップ１１に移行する。一方、再受光しない場合は、カード読み取り器からカードを取り出したかの検出を行い（ステップ１４）、カードを取り出していない場合は、コンピュータを強制的にロックアウト状態として動作を停止する（ステップ１５）。カードを取り出した場合は、ステップ１６に移行してログアウト操作を行い、コンピュータにログアウトする（ステップ１７）。一方、ステップ１１において赤外光を受光している場合は、次に、ログアウト操作がなされているかを判定し（ステップ１６）、なされていない場合は、ステップ１１に移行する。なされている場合は、ステップ１７に移行して、コンピュータにログアウトする。

【００１２】次に、図４により、本発明に係るコンピュータの情報保護方法の一実施例を示す第二の構成図を説明する。同図は、図１と同様に、ＣＰＵ１と、表示装置２と、記憶装置３と、通信制御装置４と、キーボード５と、カード６と、カード読み取り器７と、本実施例において採用したコンピュータ使用者が離席していないかどうかの検出を行なうカメラ１４とにより構成する。又、カメラ１４は、コンピュータ使用者を撮像する撮像素子１５と、撮像した画像データをＣＰＵ１において処理し易いようにディジタルデータに変換するデータ処理部１６とを備えている。又、撮像素子１５としては、ＣＣＤカメラが使用される。

【００１３】図４の動作を説明する。先ず、コンピュータにログインするまでは図１に示した第一の構成例と同様に動作し、コンピュータの使用者は、コンピュータの電源を投入してコンピュータを起動した後、ユーザＩＤ及びパスワード等の個人情報が書き込まれたカード６を、カード読み取り器７に挿入する。ＣＰＵ１は、読み取った個人情報と、記憶装置３に格納しているコンピュータの管理情報とを照合して、個人情報が登録してある管理情報に一致する場合には、コンピュータにログインさせて使用を許可する。一方、個人情報が登録してあるデータに一致しない場合は、コンピュータの使用を拒否する。又、同一カードの挿入を所定の回数行なっても個人情報と管理情報が一致しない場合は、強制ロックアウト状態としてコンピュータの動作を停止する。

【００１４】次に、コンピュータにログインすると、カメラ１４が動作を開始して撮像素子１５がコンピュータ使用者を撮影し、データ処理部１６において画像データをディジタル化処理してＣＰＵ１に入力する。ＣＰＵ１においては、入力した画像データから標準となる画像データを生成記憶しておく。カメラ１４は、コンピュータ使用者の顔面がフレーム全体に収まるよう調整し、記憶する画像データは、画像全体ではなく、肌の色、目、口の位置等大まかな情報であってもよい。そこで、一定周期でカメラ１４によりコンピュータ使用者を撮影し、コンピュータ使用者が離席したかどうかを、画像データの

変化により検出する。変化の検出は、ログイン時に記憶した標準画像データとの差分を計算し、差分がしきい値を超えたかどうかで行なう。その結果、ＣＰＵ１は、コンピュータ使用者がコンピュータ席を離席していることを確認すると、可聴音等により警報を発する。この時、コンピュータ使用者が、一定時間内にコンピュータ席に着席するかカード６をカード読み取り器７から取り出す等の適切な処置を行なわない場合は、コンピュータを強制的にロックアウトさせ、コンピュータの動作を停止する。尚、停止後のコンピュータは、コンピュータ管理者の操作により復旧させる。

【００１５】図５は、本発明に係るコンピュータの情報保護方法の一実施例を示す第二の外観図で、デスクトップ型コンピュータに実施した例である。同図は、ＣＰＵと記憶装置と通信制御装置とを内蔵したコンピュータ本体１２と、表示装置２と、キーボード５と、カード読み取り器７と、カメラ１４と、コンピュータ使用者１３とにより構成する。

【００１６】図６は、本発明に係るコンピュータの情報保護方法の一実施例を示す第二の構成図について動作を示すフローチャートである。同図を説明すると、ステップ９までは図３に示した第一の構成例と同様に動作し、コンピュータ使用者は、コンピュータを起動した後（ステップ１）、カードをカード読み取り器に挿入する（ステップ２）。コンピュータは、カードに書き込まれている個人情報のユーザＩＤが、コンピュータに予め登録してある管理情報と一致するかの判定を行い（ステップ３）、一致していない場合は、カードをカード読み取り器から強制的に排出する（ステップ４）。次に、同一カードの排出回数をカウントし、所定の回数カウントした際は（ステップ５）、ロックアウトに移行してコンピュータの動作を停止する（ステップ６）。一方、一致している場合は、ステップ７に進み、カードに書き込まれている個人情報のパスワードが、コンピュータに予め登録してある管理情報と一致するかの判定を行い、一致していない場合は、カードをカード読み取り器から強制的に排出する（ステップ４）。次に、同一カードの排出回数をカウントし、所定の回数カウントした際は（ステップ５）、ロックアウトに移行してコンピュータの動作を停止する（ステップ６）。一致している場合は、コンピュータにログインして（ステップ８）、利用を開始する（ステップ９）。

【００１７】次に、コンピュータの利用を開始すると、カメラは撮影を開始して標準画像のデータを作成し、コンピュータに記憶する（ステップ１０）。その後、コンピュータは、画像変化の有無を検出するため、標準画像のデータと現在撮影中の画像データとを比較して、その差がしきい値を超えたかどうかを判定する（ステップ１１）。画像変化が起き、画像の比較データがしきい値を超えた場合は、コンピュータ使用者がカードをカード読み取り器に挿入したまま離席したことを認識し、可聴音等の警報を発して（ステップ１２）所定の時間内に前記比較データがしきい値以下になるかどうかを判定する（ステップ１３）。そこで、コンピュータ利用者が着席することにより、画像の比較データがしきい値以下と判定した場合は、ステップ１１に移行する。一方、しきい値を超えたままの場合は、カード読み取り器からカードを取り出したかの検出を行い（ステップ１４）、カードを取り出していない場合は、コンピュータを強制的にロックアウト状態として動作を停止する（ステップ１５）。カードを取り出した場合は、ステップ１６に移行してログアウト操作を行い、コンピュータにログアウトする（ステップ１７）。一方、ステップ１１において前記比較データがしきい値以下の場合は、次に、ログアウト操作がなされているかを判定し（ステップ１６）、なされていない場合は、ステップ１１に移行する。なされている場合は、ステップ１７に移行して、コンピュータにログアウトする。

【００１８】

【発明の効果】本発明は上述したように、請求項１、２、３、４、５、６共に、コンピュータ使用者が、カード読み取り器にカードを挿入したまま離席した際に、コンピュータが不正使用されないよう対策するものであり、個人情報を格納した媒体の放置を防止する上で著しい効果を発揮する。

【図面の簡単な説明】

【図１】本発明に係るコンピュータの情報保護方法の一実施例を示す第一の構成図である。

【図２】本発明に係るコンピュータの情報保護方法の一実施例を示す第一の外観図である。

【図３】本発明に係るコンピュータの情報保護方法の一実施例を示す第一の構成図について動作を示すフローチャートである。

【図４】本発明に係るコンピュータの情報保護方法の一実施例を示す第二の構成図である。

【図５】本発明に係るコンピュータの情報保護方法の一実施例を示す第二の外観図である。

【図６】本発明に係るコンピュータの情報保護方法の一実施例を示す第二の構成図について動作を示すフローチャートである。

【図７】従来から用いられているコンピュータの情報保護方法を示す構成例である。

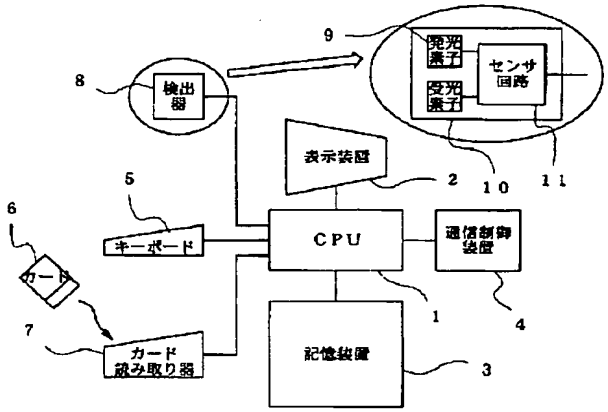
【符号の説明】

１・・ＣＰＵ、　２・・表示装置、
３・・記憶装置、　４・・通信制御装置、
５・・キーボード、　６・・カード、
７・・カード読み取り器、　８・・検出器、
９・・発光素子、　１０・・受光素子、
１１・・センサ回路、　１２・・コンピュータ本体、
１３・・コンピュータ使用者、　１

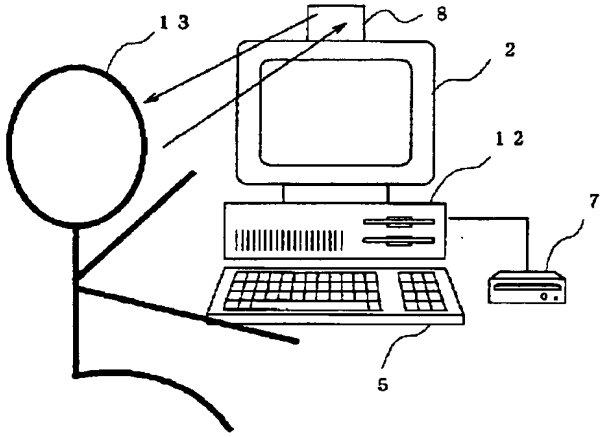
9　　10

４・・カメラ、１５・・撮像素子、　　１＊　＊６・・データ処理部

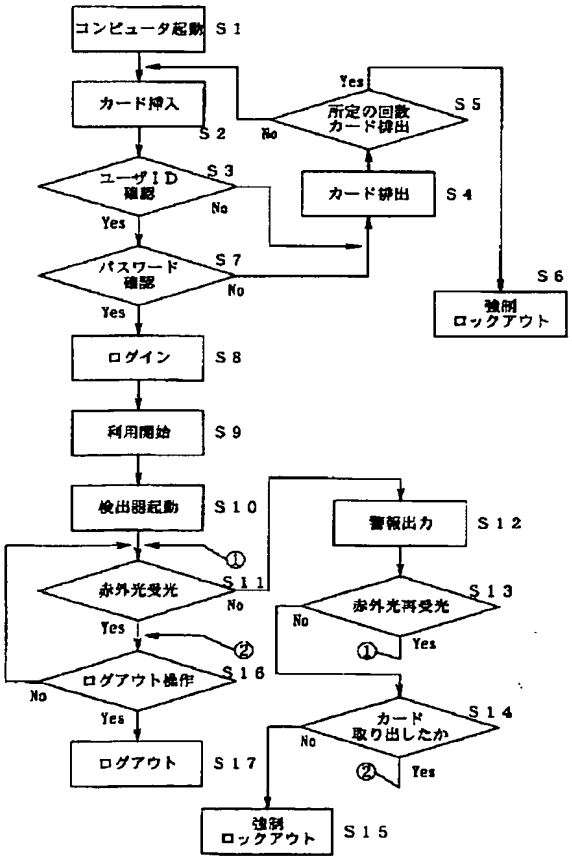
【図１】



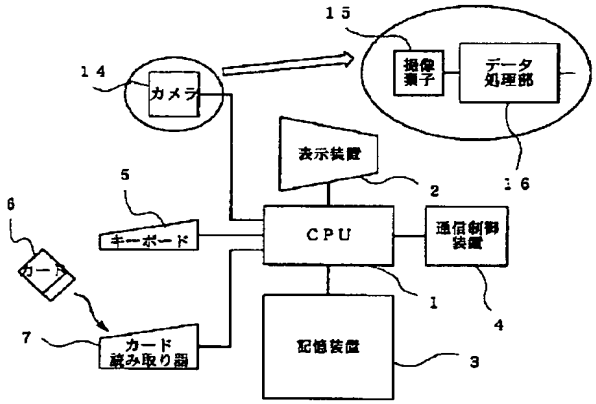
【図２】



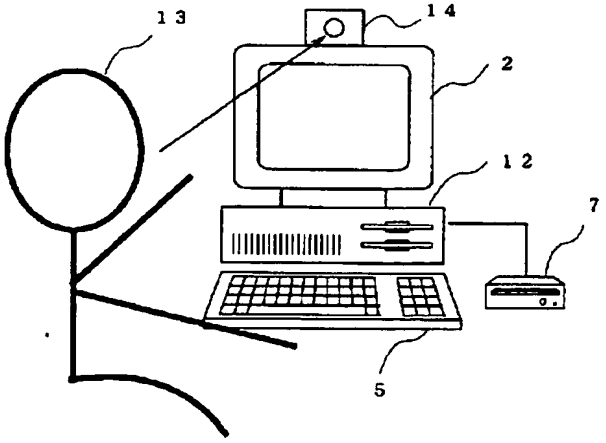
【図３】



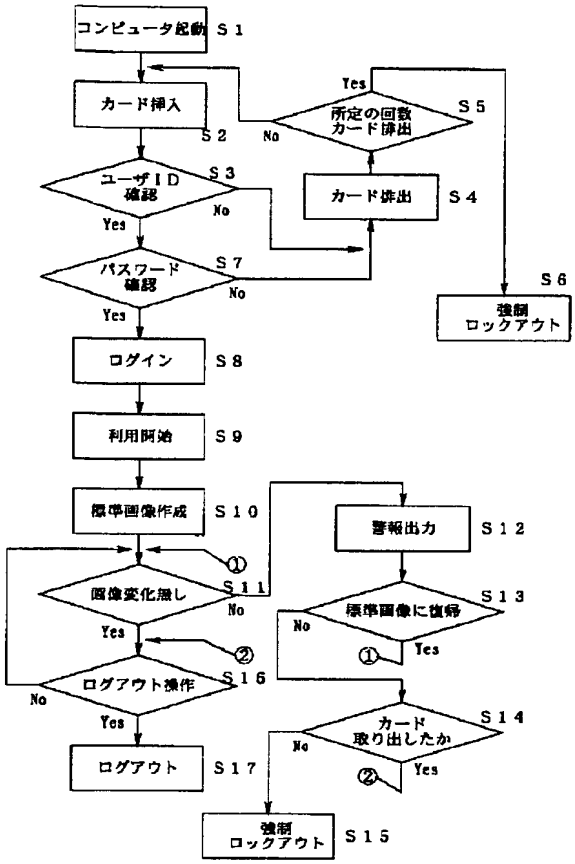
【図４】



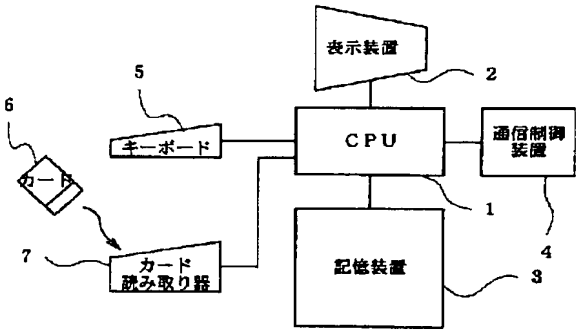
【図５】



【図６】


コンピュータ起動
S１
カード挿入
S２
所定の回数カード排出
S５
Yes
No
ユーザＩＤ確認
S３
No
Yes
カード排出
S４
パスワード確認
S７
No
Yes
S６
強制ロックアウト
ログイン
S８
利用開始
S９
標準画像作成
S１０
①
画像変化無し
S１１
No
Yes
②
ログアウト操作
S１６
No
Yes
ログアウト
S１７
警報出力
S１２
標準画像に復帰
S１３
No
①
Yes
カード取り出したか
S１４
No
②
Yes
強制ロックアウト
S１５

【図７】


表示装置
2
5
6
キーボード
CPU
通信制御装置
カード
1
4
7
カード読み取り器
記憶装置
3